BY ORDER OF THE COMMANDER
4TH FIGHTER WING

SEYMOUR JOHNSONAFBI33-152

13 SEPTEMBER 2013

Communications and Information

UNIVERSAL SERIAL BUS (USB) DEVICE POLICY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 4 CS/SCXS

Certified by: 4 CS/CC
(Major Eric W. Crowell)

Pages: 6

The purpose of this Instruction is to establish local guidelines for the acquisition and use of devices which connect via USB to resources on the AF Network. It also serves to clarify and define the role of authorized government computer users in protecting the AF Enterprise Network/Global Information Grid, through compliance with the collective policies and instructions put forth by Air Force Manual (AFMAN) 33-152, User Responsibilities And Guidance For Information Systems, AFMAN 33-282, Computer Security (COMPUSEC), and DISA STIG, Removable Storage and External Connection Technologies v1, r2, dated 28 January 2011. This Air Force Instruction (AFI) applies to all military, Department of Defense (DoD) civilian, contract, and volunteer personnel assigned to or employed at Seymour Johnson AFB who have access to the AF Network, including Air Force Reserve Command (AFRC) and Air National Guard (ANG) units in Federal status.

Failure to observe prohibitions and mandatory provisions of this Instruction in paragraph 1.2 by military personnel is a violation of Article 92, Uniform Code of Military Justice (UCMJ). Violations may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

Users will ensure that any official records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at

https://www.my.af.mil/afrims/afrims/afrims/rims.cfm. Contact supporting records managers as required. Refer recommended changes and questions to the Office of Primary Responsibility (OPR) using AF Form 847, Recommendation for Change of Publication, to 4th Communications Squadron Wing Information Assurance Office (4 CS/SCXS), 1195 Jabara Avenue, Seymour Johnson AFB, NC 27531.

SUMMARY OF CHANGES

This is an initial publication and must be read in its entirety.

1. General Information.

1.1. All personnel who access AF Networks [Non-Secure Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet), etc.], to include, but not limited to military, civilian, contractors, and summer hires, WILL NOT attach any unauthorized USB device, regardless of ownership of that device, into any SJAFB Networked Computer. This prohibition specifically disallows the plugging in of USB devices even if only to charge a battery. Further, remote users will not plug USB devices into a computer that connects to the AF Network via Virtual Private Network (VPN). Approval for authorized USB devices will be obtained from the user's Unit Information Assurance Officer (IAO).

1.2. Access to any Seymour Johnson Information System is a privilege and continued access is contingent on personal conduct. User conduct that is inconsistent with IA policies and guidelines may result in immediate suspension of access to unclassified and classified Info Systems, as well as confiscation and possible destruction of personal hardware. Additionally, military personnel, who do not comply with paragraph 1.1, including members of the Air Force Reserve Command on active duty or on inactive duty for training and the Air National Guard in Federal status, may be punished under the Uniform Code of Military Justice, Article 92, Failure to Obey Order or Regulation. Department of Defense (DoD) Civilian personnel, who do not comply, may be subjected to administrative actions in accordance with current directives. Violations by contractor personnel will be reported to the contracting office for disposition according to the terms of the contract.

1.3. Prior to obtaining access to the AF Network, all users are required to sign an AF Form 4394, Air Force User Agreement Statement - Notice and Consent Provision. In this form, users agree that "[a]t any time, the government may inspect and/or seize data stored on this information system." This consent extends to the data stored on any device attached to this information system.

1.4. USB devices subject to this inspection or seizure include, but are not limited to: memory sticks, smart phones, tablets, external hard drives, MP3 players and cameras.

1.5. The exceptions to this rule are: 1) approved USB external hard drives, and 2) USB devices with absolutely no internal memory, such as mice and keyboards. Prior to using a USB device under these exceptions, users should contact their unit IAO to verify that the device is documented as approved for use, or the device is confirmed to have no internal memory.

2. External Hard Drive Procurement.

2.1. Procurement of external hard drives for use on the AF Network must be coordinated with 4 CS/SCOS, Equipment Control Office, to obtain purchase authorization and control number.

2.2. External solid state drives are prohibited because they are essentially large capacity flash memory devices. A solid state drive is different from a standard external drive in that it has no moving parts and makes no noise or vibrations while the device is in operation. In contrast, standard hard drives have a spinning disk platter that can be heard or emits vibrations that can be felt during operation.

2.3. Unit IAOs can obtain guidance on approved external hard drives from the Wing IA Office (4 CS/SCXS). Once an approved external hard drive is properly procured, the customer's Unit IAO must establish proper approval documentation prior to use.

2.4. Documented approval will be maintained using designated electronic Unit IAO continuity folders hosted on the SJ Information Assurance (IA) Community of Practice (CoP). (**https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=AC-SC-00-82**). An Approved External Hard Drive template spreadsheet is available on the site to ensure standardized approval documentation. Access to continuity folders is limited to appointed Unit IAOs.

3. How to Approve a USB Device for Unclassified Network Use.

3.1. The only USB device authorized for use in a government computer is a government-purchased, spinning disk (non-flash memory) style hard drive. However, prior to use, qualifying government-purchased hard drives must first be approved through the Unit IAO. In those cases where government-purchased external drives are brought in from another base, it MUST be documented by the Unit IAO to establish approval for use at SJAFB.

3.2. IAW the Removable Storage and External Connection Technologies Security Technical Implementation Guide (STIG), the Unit IAO will maintain an approved USB external hard drive listing. IAOs must make their unit's Approved External Hard Drive Listing available to the 4 CS/SCXS Wing IA Office.

3.3. Once approved, all authorized USB devices must be labeled with a classification label, indicating the highest classification level of the material contained on the device, an ADP Data Descriptor Label, and a Privacy Act label as needed.

3.4. Removable media with sensitive information may not be removed from protected workplaces unless an approved operational need drives the requirement. Contact the IAO for specific guidance. Privately-owned information systems contaminated with unencrypted CUI or PII will be subject to confiscation and sanitization.

3.5. Unit IAOs may obtain guidance from 4 CS/SCXS, Wing IA Office, as needed, on the required Unit IAO Approval and Documentation process.

4. Security Actions for Unauthorized USB Use.

4.1. Users WILL NOT connect privately-owned media or peripheral devices (including, but not limited to, music/video CD/DVDs players, i-devices, commercial MP3 players, and Universal Serial Bus [USB] drives) to AF Information Systems/Government Furnished

Equipment. Violations of this policy may result in the confiscation of personal hardware. Once a user is identified to their Unit Commander as committing a violation, their account(s) will be disabled immediately. The Unit IAO will coordinate/confirm on behalf of the commander that the account is disabled. The user's Unit Commander will investigate, and if required, confiscate devices in accordance with Security Forces and AF Office of Special Investigations (AFOSI) procedures. The Unit Commander will also consider JA's advice and guidance regarding the confiscation of personal equipment. Any use of an unauthorized USB device on a classified network will result in the device/computer confiscated by the squadron and a forensics review by OSI will be conducted. If a Unit Commander/SFS/OSI/JAG has reason to suspect malicious activity is associated with a detected event and directs confiscation of a device, the 4 CS/CFP will coordinate technical assistance as needed/available to examine/sanitize the device.

4.2. The security actions taken when an unauthorized USB device is discovered connected to the network, either by electronic or physical/visual detection, are designed to regain the security posture of the SJAFB Network.

4.3. Electronic surveillance continuously monitors USB device activity on AF Networks, recording detailed information about each event. For each event where the collected data indicates a violation may have occurred, the details are compiled and provided to Unit Commanders so they can investigate the suspected violation and take administrative action against the offender if/as needed.

4.4. Reporting and/or correction of a visually detected unauthorized USB device connection is a responsibility of all users. All authorized users will protect networked and/or stand-alone Information Systems (ISs) against tampering, theft, and loss. Protect ISs from insider and outsider threats by controlling physical access to the facilities and data by implementing procedures identified in Joint, DoD, AF publications, and organizationally-created procedures. This is a clear mandate to all Users and Supervisors to be aware of the security policy concerning the network and hold each other accountable by correcting/reporting up the chain so commanders can investigate and take action as needed.

4.5. Unintentional and/or intentional actions that threaten or damage AF ISs will result in immediate suspension of access to unclassified and classified ISs according to CJCSI 6510.01. If the user disputes IS access suspension, follow local command-level legal guidance.

4.5.1. The 4 CS/CFP or Unit IAO notifies the organizational commander upon discovery or notification of user activity that is inconsistent with the terms of DoD IA training or inconsistent with approved IS security usage. At the direction of the user's organizational commander, the Unit IAO coordinates with the 4 CS/CFP to suspend user access. At a minimum, DoD IA Awareness training, and any MAJCOM required, or USCYBERCOM CTO-directed requirements will be completed prior to reinstatement of the account(s). The Unit IAO, on behalf of the organizational commander, will initiate actions to reinstate user account(s) upon the user satisfactorily completing retraining and any other requirements.

4.5.2. Only 4 CS/CFP personnel are authorized to enable an account once it is disabled for a USB violation. Unit personnel may not enable an account which has been disabled for USB violation.

4.5.3. Repeat offenders will have their account(s) immediately suspended as outlined above. However, the requirements for possible reinstatement will be elevated as deemed appropriate by coordination between the user's Unit Commander and the 4 CS Commander. Multiple repeat offenses will require coordination actions to be elevated to the 4 MSG/CC, at a minimum. Due to the security nature of the violations, commanders should consider whether or not to establish a Security Information File (SIF) through the Wing Information Protection (IP) Office. If a SIF results in suspension or loss of clearance then suspension of access may become indefinite. Refer to Table 4.1 below for recommended actions for repeat offenders.

Table 4.1. Repeat Offender Corrective Actions.

Options	1st Offense	2nd Offense	3rd Offense	4th Offense
Letter of Counseling	X			
Accomplish IA Training	X	X		
Letter of Reprimand	X	X	X	
Establish a Security Information File	X	X	X	X
Place on Control Roster/UIF			X	
Consider Article 15 / Administrative Separation				X

NOTE: This table is only illustrative and is not binding. Unit CCs exercise complete discretion in selecting responsive action(s). Commanders may use more than one action per failure. Recommend commanders consult with their local Staff Judge Advocate (SJA). Refer to the governing instructions to determine the correct form and procedures for each action.

4.6. Sanitizing unauthorized USB devices connected to the SJAFB Networks will be accomplished IAW AFMAN 33-282, Chapter 8, Remanence Security.

JEANNIE M. LEAVITT, Colonel, USAF
Commander, 4th Fighter Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMAN 33-152, User Responsibilities and Guidance for Information Systems, 1 June 2012

AFMAN 33-282, Computer Security (COMPUSEC), 27 March 2012

CJCSI 6510.01, Information Assurance and Support to Computer Network Defense, 9 February 2011

Removable Storage and External Connection Technologies STIG v1, r2, 28 January 2011

Abbreviations and Acronyms

ADP—Automated Data Processing

CFP—Communications Focal Point

CJCSI—Chairman Joint Chiefs of Staff Instruction

COMPUSEC—Computer Security

CoP—Community of Practice

CTO—Communications Tasking Order

CUI—Controlled Unclassified Information

DISA—Defense Information Systems Agency

DoD—Department of Defense

IA—Information Assurance

IAO—Information Assurance Officer

IAW—In Accordance With

IP—Information Protection

IS—Information System

MAJCOM—Major Command

PII—Personally Identifiable Information

SIF—Security Information File

STIG—Security Technical Implementation Guide

USB—Universal Serial Bus

VPN—Virtual Private Network